

UNITED STATES DISTRICT COURT

for the
Eastern District of Pennsylvania

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
location information concerning the cellular telephone
assigned call number (404) 991-1699 with International
Mobile Subscriber Identity ("IMSI") 310410175692910

Case No. 19- 1447.M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location)

See ATTACHMENT A

located in the Eastern District of Pennsylvania, there is now concealed (identify the person or describe the property to be seized):

see ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 USC § 1028(f) and (a)

18 USC § 371

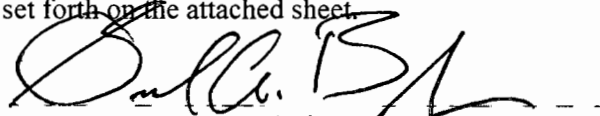
Offense Description

The application is based on these facts:

See AFFIDAVIT in support of search warrant, and certification continued on the following page.

☒ Continued on the attached sheet.

☒ Delayed notice of 30 days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Postal Inspector Samuel A. Bracken

Printed name and title

Sworn to before me and signed in my presence.

Date: 08/22/2019


Judge's signature

City and state: Philadelphia PA

Timothy R. Rice, United States Magistrate Judge

Printed name and title

See AFFIDAVIT in support of search warrant. To ensure technical compliance with 18 U.S.C. sections 3121-3127, the warrant will also function as a pen register order. I thus certify that the information likely to be obtained is relevant to an ongoing criminal investigation conducted by United States Postal Inspection Service and other agencies. See 18 U.S.C. sections 3122(b), 3123(b).

IN THE UNITED STATES DISTRICT COURT
FOR EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF
THE CELLULAR TELEPHONE ASSIGNED Case No. 19- 1447
CALL NUMBER (404) 991-1699 WITH
INTERNATIONAL MOBILE SUBSCRIBER
IDENTITY ("IMSI") 310410175692910

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Samuel A. Bracken, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A) for information about the location of the cellular telephone assigned call number (404) 991-1699, with International Mobile Subscriber Identity ("IMSI") 310410175692910 with listed subscriber **Andnet B SHIMELES**, hereinafter (the "Target Cell Phone"), whose service provider is AT&T, a wireless telephone service provider headquartered at 11760 US Highway 1, North Palm Beach, FL 33408. The "Target Cell Phone" is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

2. Because this warrant seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a "pen register" and/or "trap and trace device," *see* 18 U.S.C. § 3123(3) & (4), the requested warrant is designed to also comply with the Pen Register Act. *See* 18 U.S.C. §§ 3121-3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute. *See* 18 U.S.C. § 3123(b)(1).

3. The information sought should include, but is not limited to, data indicating the specific latitude and longitude of (or other precise location information concerning) the “Target Cell Phone” for a period of thirty (30) days.

4. I am a U.S. Postal Inspector assigned to the Philadelphia Division of the U.S. Postal Inspection Service (“Inspection Service”) and have been so employed since February 2004. My background, as well as the facts relevant to the application for search warrant, in support of which this affidavit is submitted, are laid out in the Affidavit in Support of a Criminal Complaint and Warrant to arrest **Andnet B. SHIMELES**, No. 19-1427-M, subscribed by me in the Eastern District of Pennsylvania on August 21, 2019, in connection with this case, which is hereby incorporated, in its totality, by reference as Attachment C.

5. In addition to the facts stated in Attachment C, the facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 1028(a) and 1028(f) have been committed, are being committed, and will continue to be committed by **Andnet SHIMELES**. There is also probable cause to believe that the location information described in Attachment B will constitute evidence of these criminal violations, and will lead to the identification of individuals who are engaged in the commission of these offenses and to discovery of evidence upon locating **SHIMELES**.

7. Also, based on the facts set forth in this affidavit and in Attachment C, there is probable cause to believe that **SHIMELES** has committed past violations of Title 18, United States Code, Sections 1028(a) and (f) and 371 (conspiracy to commit wire fraud and utter counterfeit securities). There is also probable cause to believe that the location information described in Attachment B will assist law enforcement in arresting **SHIMELES**, who is a “person to be arrested” within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

8. The court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is the Eastern District of Pennsylvania: a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND OF CONTINUING INVESTIGATION

9. In addition to the facts stated in Attachment C, attached, the results of the ongoing investigation in this matter have established the following facts.

10. During the course of this investigation, **SHIMELES** was found to have an active cellular telephone account with AT&T. Information obtained from AT&T revealed that **SHIMELES** opened the account with AT&T on May 20, 2016. In applying for the account, **SHIMELES** provided a billing address of 6341 Ol Madison Place, Atlanta, GA 30349, and a contact email address of andre30338@gmail.com. Further records from AT&T revealed that **SHIMELES** used a credit card number ending in xxx2504 to make 21 payments to AT&T for services on the account. It was determined that the credit card number ending in xxx2504 was issued by Capital One. AT&T records show that as of August 10, 2019, **SHIMELES** is currently assigned the Target Cell Phone, including telephone number (404) 991-1699 and IMSI 310410175692910.

11. Records obtained from Capital One revealed that **SHIMELES** applied for the credit card bearing number ending in xxx2504 on May 18, 2016, using social security number xxx-xx-5031, a date of birth matching the date of birth on **SHIMELES's** Georgia driver's license, an email address of ashimeles20784@gmail.com, a home address of 6341 Ol Madison Place, Atlanta, GA 30349, and a telephone number of (404) 991-1699, the "Target Cell Phone."

12. Records were obtained from Google for information pertaining to the following email addresses:

- Ashimeles20784@gmail.com – provided by **SHIMELES** to Capital One.
- Andre30338@gmail.com provided by **SHIMELES** to AT&T.
- James30338@gmail.com – An email address that the investigation revealed is also being used by **SHIMELES**, which was found during a search of email account stevenhoward76@yahoo.com, pursuant to a federal search warrant, and described in Attachment C.

13. Google records revealed the following information regarding the above email addresses:

- Ashimeles20784@gmail.com – This email address was created on November 25, 2011. The individual who created this account provided Google with the name **Andnet SHIMELES**, a recovery email address of andre30338@gmail.com, and a telephone number of (404) 991-1699, the Target Cell Phone. Google captured the following IP address associated with a logout from this account on July 1, 2019: 99.153.138.116.
- Andre30338@gmail.com – This email address was created on July 1, 2009. The individual who created this account provided Google with the

name Andre White and a recovery email address of ashimeles20784@gmail.com. Google captured the following IP address associated with a login to this account on July 9, 2019 at 15:46:26 UTC: 99.153.138.116.

- James30338@gmail.com – This email address was created on September 29, 2010. The individual who created this account provided Google with the name James Camron, a recovery email address of stevenhoward76@yahoo.com, and a phone number of 678-392-5887. Google captured the following IP address associated with a logout from this account on July 9, 2019 at 15:45:30: 99.153.138.116.

14. I conducted a query to determine the service provider for IP address 99.153.138.116, and discovered that this IP address belonged to AT&T Uverse, which is a residential Internet Service Provider, which provides residential high speed, broadband Internet service. A subpoena was issued to AT&T for the subscriber associated with this IP address, but AT&T has not yet provided a response.

15. Further records provided by AT&T revealed that the Target Cell Phone associated with SHIMELES's account was an Apple Iphone 6 from June 2016 to December 2018 and an Apple Iphone XS from December 2018 to August 2019.

16. Furthermore, as mentioned above and as described in Attachment C, a federal search warrant was issued for email address stevenhoward76@yahoo.com. I reviewed the sent and received emails from this account, and noticed that on the emails sent from stevenhoward76@yahoo.com, a footer was included stating the following: "Sent from Yahoo

Mail for iPhone.” This footer was included on emails sent to the eleven email addresses identified in Attachment C as being controlled by defendants in Criminal Case No. 18-291.

17. Also recovered through execution of the federal search warrant for stevenhoward76@yahoo.com, were IP addresses captured during login to the account. The search warrant was served on May 13, 2019. Records obtained show that the last login to the stevenhoward76@yahoo.com email account occurred on May 10, 2019 with a captured IP address of 99.153.138.116. This was the same IP address associated with the previously mentioned Google accounts.

18. In conclusion, it is believed that **Andnet B. SHIMELES** is operating an Apple iPhone through service provider AT&T. Records show that **SHIMELES** has been a customer of AT&T since May 2016, and during this time period has operated Apple iPhones, the first being an Apple iPhone 6 and then later an Apple iPhone XS. Furthermore, IP address records show that email addresses stevenhoward76@yahoo.com, ashimeles20784@gmail.com, andre30338@gmail.com, and james30338@gmail.com, all captured IP address 99.153.138.116, either logging in or out of the respective accounts between May 2019 and July 2019. A review of email records obtained from stevenhoward76@yahoo.com pursuant to a federal search warrant shows that in his communication with co-conspirators and other customers, **SHIMELES** was using Yahoo Mail for iPhone. This is recorded in the footer of sent messages. It is therefore believed that the Apple iPhone currently being used by **SHIMELES** will contain evidence of violations of Title 18, United States Code, Section 1028(f) Identity Theft. Additionally, an arrest warrant has been issued for **SHIMELES** and the requested information this warrant seeks will determine the approximate location of **SHIMELES**'s telephone, that is, the Target Cell Phone, (404) 991-1699, and help to effect the arrest of **SHIMELES**.

TRAINING AND EXPERIENCE

19. In my training and experience, I have learned that AT&T is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including E-911 Phase II data, also known as GPS data or latitude-longitude data and cell-site data, also known as “tower/face information” or cell tower/sector records. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device’s signal using data from several of the provider’s cell towers. Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the “sector” (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise than E-911 Phase II data.

20. Based on my training and experience, I know that AT&T can collect E-911 Phase II data about the location of the Target Cell Phone, including by initiating a signal to determine the location of the Target Cell Phone on AT&T’s network or with such other reference points as may be reasonably available.

21. Based on my training and experience, I know that AT&T can collect cell-site data about the Target Cell Phone. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1)

the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as AT&T typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

AUTHORIZATION REQUEST

22. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c).

23. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the “Target Cell Phone” would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

24. I further request that the Court direct AT&T to disclose to the government any information described in Attachment B that is within the possession, custody, or control of AT&T. I also request that the Court direct AT&T to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with AT&T's services, including by initiating a signal to determine the location of the "Target Cell Phone" on AT&T's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate AT&T for reasonable expenses incurred in furnishing such facilities or assistance.

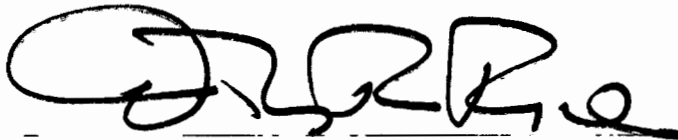
25. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the Target Cell Phone outside of daytime hours.

26. I further request that the warrant, this affidavit, and Attachment C, be sealed until further order of the Court in order to avoid premature disclosure of the investigation, guard against flight, and better ensure the safety of agents and others, except that three (3) certified copies should be made available to the United States Attorney's Office and agents of the US Postal Inspection Service for service upon AT&T.



Samuel A. Bracken
Inspector
United States Postal Inspection Service

Subscribed and sworn to before me on the 22 day of August 2019.



THE HONORABLE TIMOTHY R. RICE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

1. The cellular telephone assigned call number **(404) 991-1699**, with International Mobile Subscriber Identity 310410175692910, with listed subscriber **Andnet SHIMELES** (the Target Cell Phone), whose wireless service provider is AT&T, a company headquartered at 11760 US Highway 1, North Palm Beach, FL 33408.
2. Records and information associated with the Target Cell Phone that is within the possession, custody, or control of AT&T.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

All information about the location of the Target Cell Phone described in Attachment A for a period of thirty days, during all times of day and night. Information about the location of the “Target Cell Phone” includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information, as well as all data about which “cell towers” (i.e., antenna towers covering specific geographic areas) and “sectors” (i.e., faces of the towers) received a radio signal from the cellular telephone described in Attachment A.

To the extent that the information described in the previous paragraph (hereinafter, “Location Information”) is within the possession, custody, or control of AT&T, AT&T is required to disclose the Location Information to the government. In addition, AT&T must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with AT&T’s services, including by initiating a signal to determine the location of the “Target Cell Phone” on AT&T’s network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate AT&T for reasonable expenses incurred in furnishing such facilities or assistance.

This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

II. Information to Be Seized by the Government

All information described above in Section I that constitutes evidence of violations of Title 18, United States Code, Section 1028(a) and (f) involving **Andnet SHIMELES**.

All information described above in Section I that will assist in arresting **SHIMELES**, who is charged in a sealed complaint with violating Title 18, United States Code, Section 1028(a) and (f) and Title 18, United States Code, Section 371, issued August 21, 2019 along with an arrest warrant, also under seal at this time, who is a “person to be arrested” within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

AFFIDAVIT

I, Samuel A. Bracken, United States Postal Inspector, United States Postal Inspection Service ("Inspection Service"), being duly sworn, state the following:

1. I have been employed as a Postal Inspector with the Inspection Service for approximately fifteen years and am currently assigned to the Philadelphia Division. I am currently assigned to the Miscellaneous Crimes Team, which investigates violations of federal law, including identity fraud, aggravated identity theft, and mail fraud and wire fraud, in violation of Title 18, United States Code, Sections 1028(a), 1028A, 1341 and 1343, respectively. I have received training in investigating identity theft, credit card fraud, counterfeit check fraud, counterfeit identification card fraud, and mail and wire fraud offenses, including attending seminars and conferences hosted by the Inspection Service, the United States Department of Justice, the International Association of Financial Crimes Investigators, and various other law enforcement entities. During my employment as an Inspector, I have participated in hundreds of investigations involving identity fraud, aggravated identity theft, mail fraud and wire fraud and in addition, I have been the Inspection Service's case agent on numerous investigations involving these offenses.

PURPOSE OF AFFIDAVIT

2. The Inspection Service, the United States Secret Service ("USSS") and the Social Security Administration – Office of Inspector General ("SSA-OIG") are participating in a joint investigation of the activities of Andnet SHIMELES ("SHIMELES") and others involved with SHIMELES in a conspiracy to commit fraud in connection with false identification documents and authentication features, which were then used by SHIMELES's co-conspirators to cash and

attempt to cash thousands of counterfeit checks with a face value of over \$1,000,000 at Walmarts across the United States, from June 2016 until at least July 2018. As stated below, there is probable cause to believe that during the period June 2016 until early 2019, SHIMELES worked in concert with at least nine co-conspirators to produce, then provide to the co-conspirators, false identification documents and authentication features which the co-conspirators used to cash the counterfeit checks, in violation of Title 18, United States Code, Sections 1028(f) and (a), 371, 513 and 1343.

3. I submit this affidavit in support of an application for a warrant to arrest Andnet SHIMELES. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Because this affidavit is submitted for the limited purpose of establishing probable cause to arrest SHIMELES, this affidavit does not set forth each and every fact learned by me or other agents during the course of this investigation.

4. In my training and experience, I have learned that persons who commit financial fraud and identity fraud crimes often use false names and obtain email addresses and cellular telephones in those false names, in order to hide their identities, even from their co-conspirators. Individuals will often make it difficult to trace their fraudulent activity in order to hide their activity from law enforcement. Specifically, individuals involved in identity theft can conduct their fraud from anywhere they have access to a computer or cellular telephone. This allows them some measure of anonymity. They will often even hide their identity from co-conspirators, therefore if any co-conspirator is ever arrested, they won't be able to provide much information about who they were working with to conduct identity theft.

BACKGROUND OF INVESTIGATION

5. On December 11, 2018, a grand jury in the Eastern District of Pennsylvania returned an 18-count superseding indictment against nine defendants: Ahmad BECOATE, Jeffrey ROACH, Jethro RICHARDSON, Nathaniel JONES, Jared MILLER, JuQuan HARVEY, Robert HARRINGTON, Leander ROWELL, and Brian CHERRY. The indictment charged that beginning no later than June 2016 and continuing until at least July 2018, these defendants and others conspired and schemed to present thousands of counterfeit payroll checks, with a total face value in excess of \$1,000,000, at Walmart stores located across the United States, in violation of Title 18, United States Code, Sections 371, 1343, 513 and 1028A, and Title 42, United States Code, Section 408(a)(7)(B). The case was assigned to the Honorable Joseph F. Leeson, Jr., under Criminal No. 18-291. The case remains pending: seven of the nine defendants have pleaded guilty; four of those have been sentenced while the other three await sentencing; and the two other defendants await trial.

6. I am the Inspection Service's case agent in this investigation. During the investigation, I learned from Walmart representatives that at some Walmart store locations, Walmart permitted customers to cash payroll checks. When a customer presented a payroll check to a Walmart employee for cashing, the customer was required to enter his or her social security number ("SSN") into a keypad and provide proper identification, usually a state driver's license or identification card. The Walmart employee scanned the check through a check reader. Certain information, including the account number of the bank account on which the payroll check was drawn; the drawee bank's routing number; and the SSN provided by the customer, was transmitted via interstate wire transmission from the Walmart store's computer system to the

computer servers of a contractor for Walmart. The contractor's computer servers were located in Chicago, Illinois and St. Petersburg, Florida. The contractor analyzed the data provided by the check and the Walmart customer, then transmitted an interstate wire communication from its computer servers back to the Walmart store, recommending that Walmart accept, or decline, the payroll check.

7. Also during the investigation, my co-case agents and I obtained federal warrants to search eight email accounts. These email accounts belonged to defendants BECOATE, ROACH, MILLER, HARVEY, ROWELL, and RICHARDSON, and were used by those six conspirators, all of whom were eventually indicted in Criminal No. 18-291.

8. Review of those email accounts and interviews of two of the defendants in the case, who agreed to speak with the government ("D 1" and "D 2") revealed that each of the nine defendants in Criminal No. 18-291 dealt with an individual who provided the false identification documents and authentication features needed to cash the counterfeit checks. That individual was later identified as Andnet SHIMELES.

9. One of the defendants who spoke with the government ("D 1")¹ provided the following information on the individual later identified as Andnet SHIMELES.

¹ D 1 is currently incarcerated in the present case, Criminal No. 18-291. Not counting this case, D 1 has six prior felony convictions for various non-violent offenses, starting in 2008. For two of the felony convictions D 1 received suspended sentences. D 1 was sentenced to serve prison time for each of the other four convictions. His sentences ranged from a low end of 10 months to a high end of 32 months. D 1 has no federal convictions. In 2014, D 1 was convicted of felony identity theft and sentenced to 19 to 32 months in prison followed by two years of probation. D 1 was on supervision in that 2014 case while he was a member of the conspiracy charged in Criminal No. 18-291. D 1 has pleaded guilty in Criminal No. 18-291, pursuant to a cooperation plea agreement and awaits sentencing, at which D 1 hopes to receive a lower sentence than the approximately 46 to 57 month sentencing guideline range, plus 24-month consecutive sentence for aggravated identity theft, that D 1 would face absent a downward departure motion from the government. No promises have been made to D 1 about whether or not the government will file such a motion. To date, the information that D 1 has provided has been found reliable and has been corroborated by other evidence.

- D 1 stated that the false identification cards used by himself and others to cash the counterfeit checks came from an individual in the Atlanta, GA area whom he knew as “Andy.” D 1 advised that he paid “Andy” approximately \$150 to \$175 per false identification card, and paid “Andy” by sending money via Western Union. D 1 stated that at “Andy’s” direction, he would send the money via Western Union to “Cory Wright” or “Chris Wright,” though D 1 stated that he didn’t believe this to be “Andy’s” real name. D 1 stated that he would order a false identification card from “Andy” by sending “Andy” an email requesting a “face.” D 1 advised agents that the email address through which he communicated with “Andy” was “stevenhoward,” or something close to that, at yahoo.com. D 1 estimated that at least five of the co-defendants in this case obtained their false identification cards from “Andy.” During a second interview, D 1 added further details, reiterating D 1’s previous statement and also telling agents that he had met “Andy” on one occasion, in 2011 or 2012, at the Varsity Restaurant in Atlanta, GA. D 1 described “Andy” as a light-skinned black male, approximately 5’10” tall, slender build, with dreadlocks.

10. A second defendant (“D 2”)² provided the following information concerning the individual who provided the false identification cards needed to cash the counterfeit checks, which individual was later identified as Andnet SHIMELES:

² D 2 is serving a sentence of 94 months in the present case, Criminal No. 18-291. In addition, D 2 has five prior felony convictions for fraud and theft offenses, starting in 2008. For those prior felony convictions, D 2 received sentences ranging from 10-12 months incarceration to 15-18 months incarceration. D 2 pleaded guilty in this case under a non-cooperation plea agreement and was sentenced on July 23, 2019. No promises were made to D 2 concerning whether the government would file a motion for reduction of sentence under Rule 35, Fed.R.Crim P. To date, the information that D 2 has provided has been found reliable and has been corroborated by other evidence.

- D 2 stated that the false identification cards came from an individual named “Chris Wright” in Atlanta, GA. D 2 advised that he communicated with “Wright” via an email address, “stevenhoward@yahoo.com,” and that he would request a false identification card with an email requesting a “face.” D 2 stated that he also communicated with “Wright” via text messaging on his cellular telephone. D 2 stated that contact information for “Wright” was saved in his phone as “BMAN.” D 2 stated that “Wright” charged approximately \$150 per false identification card plus a \$25 overnight shipping charge. D 2 advised that he paid “Wright” via MoneyGram sent to the Atlanta, GA area.

11. As stated above in paragraph 7, as part of the investigation, my co-case agents and I obtained and executed warrants to search eight email accounts belonging to defendants BECOATE, ROACH, MILLER, HARVEY, ROWELL, and RICHARDSON. Analysis of the material obtained through the searches of the eight email accounts showed that these accounts contained PII, including PII that had been used in passing counterfeit checks at Walmart locations. Analysis also showed that five of these eight accounts had communicated with the email address stevenhoward76@yahoo.com in order to obtain false identification documents to further the scheme of cashing counterfeit checks. The emails to stevenhoward76@yahoo.com showed the defendants requesting false identification documents, most often drivers’ licenses of various states; providing information relating to payment for the false identification documents; and requesting that the false identification documents be sent by Federal Express to various locations in the United States. These false identification documents were later used by the defendants to cash counterfeit checks at Walmart locations throughout the United States,

including Walmarts located in the Eastern District of Pennsylvania.

12. On May 13, 2019, federal search warrant No. 19-831-M was issued for a Yahoo email account bearing the name **stevenhoward76@yahoo.com**. The warrant was issued by the Honorable Carol Sandra Moore Wells, United States Magistrate Judge for the Eastern District of Pennsylvania, and served on Yahoo, aka Oath Holdings Inc.

13. On June 19, 2019, your affiant received a response from Yahoo regarding the search warrant. Yahoo provided a CD containing the responsive documents.

14. Review of the email address **stevenhoward76@yahoo.com** showed that from June 2016 through May 2019, approximately 36 different email addresses communicated with **stevenhoward76@yahoo.com**, with the majority of the emails discussing the ordering of false identification documents; how much, how and where to send payment for the orders; whether the false identification documents had been shipped or not; and tracking numbers associated with the orders.

15. Review of the **stevenhoward76@yahoo.com** email address showed that out of the 36 total email accounts that communicated with **stevenhoward76@yahoo.com**, eleven email addresses were controlled by the defendants charged in Criminal Case No. 18-291. Those email accounts and the defendants who used them are listed below:

- **Crazyswagg87@gmail.com** – Ahmad Becoate
- **Mall3412@aol.com** -- Ahmad Becoate
- **Bamz85@icloud.com** -- Jeffrey Roach
- **Bamz85aga@gmail.com** -- Jeffrey Roach
- **Jeffreyroach1985@gmail.com** -- Jeffrey Roach

- J_black009@yahoo.com – Jeffrey Roach
- Mochaboy69@gmail.com – Leander Rowell
- Leebenjamin82@yahoo.com – Leander Rowell
- Jlmiller1286@gmail.com – Jared Miller
- Cherry.brian51@gmail.com – Brian Cherry
- Chickken01@gmail.com -- Nathaniel Jones

16. I know that the above eleven (11) listed email addresses belong to the six named defendants, through search warrants executed on six of the above email addresses; search warrants executed on cellular telephones obtained during the course of the investigation; travel records related to the defendants; and through review of the content of the email messages back and forth between the email addresses and **stevenhoward76@yahoo.com**.

17. Although the email address **stevenhoward76@yahoo.com** was registered in the false name “Steven Howard,” and while D 1 and D 2 explained to the agents that the false ID maker did not give them his full name, and in fact appeared to use several different names, our investigation eventually identified the false ID maker as Andnet SHIMELES, as detailed below.

18. Investigation shows that when ordering the false identification documents and authentication features (that is, false driver’s licenses and identification cards), these defendants sent the email address **stevenhoward76@yahoo.com** photographs to be placed on the false identification documents and authentication features. The defendants usually requested that the photograph be placed on a template of a driver’s license for a particular state. As detailed below, after payment had been made, Andnet SHIMELES sent to the defendant, by overnight

delivery, a false driver's license of the state that had been ordered, containing the photograph along with counterfeited holograms or watermarks of the particular state. The defendants referred to such a false identification document/authentication feature as a "face." The defendants then used computer printers to paste personal identifying information ("PII") of innocent persons onto the false drivers' licenses, in order to be able to reuse them when cashing counterfeit checks at various Walmarts.

19. From my training and experience; from interviewing witnesses in this case; and from review of the attachments to emails in **stevenhoward76@yahoo.com**, I believe that the items that SHIMELES shipped to the defendants constitute "false identification documents" and "authentication features" within the meaning of the identity fraud statute, Title 18, United States Code, Section 1028(d)(4) and (d)(1) respectively.

IDENTIFICATION OF ANDNET SHIMELES AS THE FALSE ID MAKER

20. During the course of the investigation, D 2's cellular telephone was seized as evidence and searched pursuant to federal warrant. A review found text message communications with an individual saved as "BMAN" with a telephone number of **404-426-6144**. 404 is an area code assigned to the Atlanta GA area. Subscriber records for cellular telephone number **404-426-6144** showed that this number has been registered in the following name since August 5, 2013:

- **Subscriber Name:** Steven Howard
- **Subscriber Email:** **Stevenhoward76@yahoo.com**

The records obtained showed that cellular telephone number **404-426-6144** was still active as of May 2019. The records showed that this telephone number belonged to a prepaid account.

21. On May 13, 2019, search warrant No. 19-830-M was issued by the Honorable Carol Sandra Moore Wells, United States Magistrate Judge for the Eastern District of Pennsylvania. That warrant authorized seizure of call detail records, cell phone tower usage, and Per Call Measurement Data (PCMD) for telephone number **404-426-6144** belonging to Sprint. PCMD is data collected by Sprint related to the distance a cell phone signal travels from the phone to the nearest cellular tower. In the case of Sprint, and the PCMD data, Sprint can provide an approximate location when the target cellular telephone is in use. PCMD data is not recorded and saved by Sprint on every call.

22. Analysis of the cellular phone records for **404-426-6144** revealed that Sprint was able to capture PCMD data for two cellular telephone calls for **404-426-6144**. The following was the information provided by Sprint for these captures:

- April 23, 2019 – Sprint captured PCMD data for **404-426-6144** using a cellular telephone tower located at Latitude 33.583725 and Longitude -84.46971 with an approximate distance from tower to phone of .74 miles. I conducted a location query for Latitude 33.583725 and Longitude -84.46971 and found it was located at an approximate address of 6175 Old National Highway, Atlanta, GA 30349.
- April 24, 2019 – Sprint captured PCMD data for **404-426-6144** using a cellular telephone tower located at Latitude 33.579346 and Longitude -84.469164 with an approximate distance from tower to phone of .78 miles. I conducted a location query for Latitude 33.579346 and Longitude -84.469164 and found it located at an approximate address of 6396 Old National Highway, Atlanta, GA 30349.

23. Analysis of the cell phone records for **404-426-6144** revealed that Sprint was able to capture cellular telephone tower usage on numerous calls using **404-426-6144**. Sprint was not able to capture this data on all calls, but significantly more than the PCMD information collected. A review showed **404-426-6144** was using cellular tower #1546 frequently from January 2019 through April 2019. Sprint provided records showing cellular tower #1546 located at Latitude 33.587597 and Longitude -84.46811. I conducted a location query for Latitude 33.587597 and Longitude -84.46811 and found it located at an approximate address of 6120 Old National Highway, Atlanta, GA 30349.

**WESTERN UNION, MONEYGRAM, RIA FINANCIAL
AND OTHER FORMS OF PAYMENT**

24. Records were obtained from Western Union, MoneyGram, and RIA Financial showing payments from the nine defendants to “Chris Wright” and “Mark Brown,” as directed by the **stevenhoward76@yahoo.com** email account. A review of records from Western Union, MoneyGram, and RIA Financial revealed that between August 2013 and August 2018, the nine defendants sent approximately 110 payments to the false names “Chris Wright” and “Mark Brown,” which totaled approximately \$23,252. In addition, one known payment was sent via a “cash app” by defendant Leander ROWELL for \$400 in February 2019. Additional payments were also sent to the operator of the **stevenhoward76@yahoo.com** email account in the names “Chris Wright” and “Mark Brown” by other customers identified through email, Western Union, MoneyGram, and RIA Financial records.

25. A review of the **stevenhoward76@yahoo.com** email account revealed a .pdf file being forwarded from **stevenhoward76@yahoo.com** to another email address, **andre30338@gmail.com**, with the name “Andre SHIMELES” as the recipient. Public records

show that SHIMELES previously lived at 3102 Dunwoody Gables Drive, Atlanta, GA, which is located in the 30338 zip code. The forwarded .pdf file was a Capital One credit card statement for December 2019 for credit card number xxx2504 in the name of Andenet B SHIMELES, 6341 Ol Madison Pl, Atlanta, GA 30349.

26. Records obtained from Capital One revealed that credit card number xxx2504 was applied for by SHIMELES on May 18, 2016, using social security number xxx-xx-5031, a date of birth matching the date of birth on SHIMELES's Georgia driver's license, email address ashimeles20784@gmail.com, and a home address of 6341 Ol Madison Place, Atlanta, GA 30349. Public records show that SHIMELES previously lived at 8308 Oliver Street, New Carrollton, MD, a location in the 20784 zip code.

27. Further records obtained from Capital One revealed that credit card number xxx3080 was applied for by SHIMELES on June 16, 2019, using that same social security number, xxx-xx-5031, the same date of birth, email address ashimeles20784@gmail.com, and a home address of 6341 Ol Madison Place, Atlanta, GA 30349.

28. Records obtained from Capital One revealed that credit card number xxx2504 in the name of SHIMELES was being used for payments to AT&T. I obtained records for SHIMELES from AT&T; those records showed that SHIMELES was a current wireless subscriber with AT&T. AT&T records show that SHIMELES began service with AT&T in May 2016 and provided AT&T with a contact email address of andre30338@gmail.com. This is the same email address that the forwarded Capital One statement was sent to from the **stevenhoward76@yahoo.com** email address. The current phone number identified for SHIMELES on this account was 404-991-1699. The current address on the account is 6341 Ol

Madison Place, Atlanta, GA 30349, SHIMELES's residence.

29. I conducted an NCIC query on Andnet SHIMELES and discovered that SHIMELES has been arrested in Georgia and Maryland for various fraud related offenses including identity theft, check forgery, and credit card fraud. On April 1, 2014, SHIMELES was convicted in Georgia of two counts of third degree forgery and two counts of second degree forgery, for which he received a sentence of five years' probation and a \$6,000 fine. I reviewed a booking photograph of SHIMELES from an arrest on November 9, 2009 by the Dunwoody, GA Police Department and observed SHIMELES to be a light-skinned black male, identified as approximately 6 feet tall and approximately 150 pounds. In the booking photograph, SHIMELES wore his hair in distinctive long dreadlocks.

30. As previously described by D 1, the "Andy" whom D 1 met in 2010 or 2011 at the Varsity Restaurant in Atlanta was a light skinned black male, approximately 5'10" tall, slender build, with dread locks. This description matches the appearance of SHIMELES in the Dunwoody GA booking photograph.

31. I have also reviewed property records of the residence of Andnet SHIMELES, 6341 Ol Madison Place, Atlanta, GA. Those records show that this property was purchased by SHIMELES in December 2009. This address is located within approximately 3/4 of a mile from where Sprint captured the PCMD during the phone calls from **404-426-6144**. Also, the Sprint cellular telephone tower most used by **404-426-6144** is located within approximately 3/4 of a mile from SHIMELES's residence. Also, located within miles of this residence were several of the locations where money was sent via Western Union, MoneyGram, and RIA Financial by the aforementioned defendants and picked up by a person using the name "Chris

Wright,” including a Kroger location at 4550 Jonesboro Road, Union City, GA (approximately five miles from SHIMELES’s residence) and a Walmart located at 6149 Old National Highway, Atlanta, GA 30349 (approximately .75 miles from SHIMELES’s residence).

32. I obtained a work history summary of SHIMELES from the United States Department of Labor, and discovered that SHIMELES was employed during all of 2018 and 2019 at Punch Bowl Social, located at 875 Battery Avenue SE, Atlanta, GA 30339. This employment address is located within approximately two miles of a Walmart at 1785 Cobb Parkway SE, Marietta, GA 30067, again a location where funds were picked up by a person using the name “Chris Wright” via MoneyGram and RIA Financial, in payment for purchases of false identification documents and authentication features by the defendants.

33. Of the 110 payments by the nine defendants in Criminal No. 18-291, 106 of those payments were to the locations listed below:

RIA Financial – Walmart at 6149 Old National Highway, College Park, GA -- 10 pickups (.7 miles from residence)

RIA Financial – Walmart at 4735 Jonesboro Road, Union City, GA – 11 pickups (5.9 miles from residence)

RIA Financial – Walmart at 844 Cleveland Avenue, East Point, GA – 3 pickups (9.6 miles from residence)

RIA Financial – Walmart at 7050 Highway 85, Riverdale, GA – 7 pickups (5.1 miles from residence)

RIA Financial -- Walmart at 1785 Cobb Parkway South, Marietta, GA – 2 pickups (2.1 miles from work)

Moneygram -- Walmart at 6149 Old National Highway, College Park, GA – 12 pickups (.7 miles from residence)

Moneygram – Walmart at 844 Cleveland Avenue, East Point, GA – 6 pickups (9.6 miles

from residence)

Moneygram -- Walmart at 1785 Cobb Parkway South, Marietta, GA -- 2 pickups (2.1 miles from work)

Moneygram -- Walmart at 7050 Highway 85 Riverdale, GA -- 2 pickups (5.1 miles from residence)

Moneygram -- CVS at 7055 Old National Highway, Riverdale, GA -- 17 pickups (1.4 miles from residence)

Moneygram -- Walmart at 4735 Jonesboro Road, Union, City, GA -- 11 pickups (5.9 miles from residence)

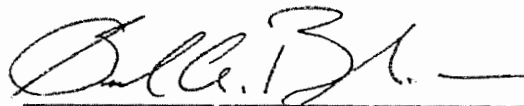
Western Union -- Kroger at 6055 Old National Highway, College Park, GA -- 16 pickups (.9 miles from residence)

Western Union -- Kroger at 4550 Jonesboro Road, Union City, GA -- 7 pickups (5.4 miles from residence)

CONCLUSION

34. Based on the information contained in this affidavit, your affiant respectfully submits that

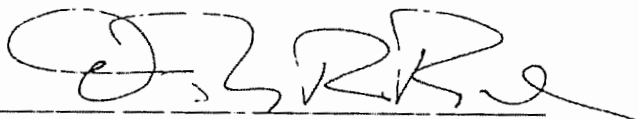
there is probable cause to believe that SHIMELES has violated Title 18, United States Code, Section 1028(f) (conspiracy to commit fraud in connection with identification documents and authentication features); Title 18, United States Code, Section 1028(a) (producing, transferring and using false identification documents and authentication features); and Title 18, United States Code, Section 371 (conspiracy to commit wire fraud and utter counterfeit securities). Accordingly, your affiant respectfully requests that this Court issue a warrant to arrest Andnet SHIMELES for violations of 18 U.S.C. §§ 371, 1028(f) and 1028(a).



SAMUEL A. BRACKEN
Postal Inspector
United States Postal Inspection Service

SWORN TO AND SUBSCRIBED

BEFORE ME, this 21
day of August, 2019:



THE HONORABLE TIMOTHY R. RICE
United States Magistrate Judge